



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

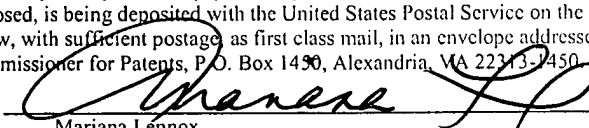
Application No.: <b>10/701,029</b>	Examiner: <b>Eleni A. Shiferaw</b>
Applicant: <b>Brian Grove et al.</b>	Art Unit: <b>2436</b>
Filed: <b>November 4, 2003</b>	Confirmation No.: <b>6164</b>
Customer No.: <b>23973</b>	Attorney Docket No.: <b>200634-0029-00-US (408195)</b>
Title: <b>SECURE AUTHENTICATION USING HARDWARE TOKEN AND COMPUTER FINGERPRINT</b>	

**Mail Stop: Appeal Brief – Patents**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**APPEAL BRIEF**

Sir:

This Appeal Brief is being submitted in response to the Advisory Action that was mailed on April 7, 2009 in the above-identified application. A Notice of Appeal and appropriate fees are filed herewith. If any fee is determined to be paid incorrectly, please charge the correct fee or credit any overpayment to Deposit Account 50-0573.

<p style="text-align: center;"><b>CERTIFICATE OF MAILING</b> <b>UNDER 37 C.F.R. 1.8(a)</b></p> <p>I hereby certify that this paper, along with any paper referred to as being attached or enclosed, is being deposited with the United States Postal Service on the date indicated below, with sufficient postage, as first class mail, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.</p> <p>BY <u></u> Mariana Lennox</p> <p>DATE: <u>April 22, 2009</u></p>
--

04/27/2009 CCHAU1 00000050 10701029

02 FC:1402

540.00 OP

## **1. REAL PARTY IN INTEREST**

The instant application has been assigned to:

SafeNet, Inc.  
4690 Millennium Drive  
Belcamp, Maryland 21017

SafeNet, Inc. is the real party in interest for this application.

## **2. RELATED APPEALS AND INTERFERENCES**

There are no other appeals or interferences currently pending that are related to this application.

## **3. STATUS OF CLAIMS**

Claims 1-34, 36-49, 51-64, and 66-78 are currently pending. Claims 1-33 were withdrawn in response to a restriction requirement. Claims 35, 50, and 65 have been canceled. Claims 34, 36-49, 51-64, and 66-78 stand rejected in this application. All presently rejected claims have been rejected at least twice, and are the subject of this appeal. The Claims Appendix includes all currently pending claims.

## **4. STATUS OF AMENDMENTS**

No amendments have been filed subsequent to the most recent rejection.

## **5. SUMMARY OF CLAIMED SUBJECT MATTER**

The claims to be argued on appeal include independent method claim 34 and its dependent claims 36-48; independent apparatus claim 49 and its dependent claims 51-63; and

independent apparatus claim 64 and its dependent claims 66-78. Accordingly, those claims are summarized below. References to the application are to the application as originally filed.

The claims are directed to preventing unauthorized access to a secure computing system that can be accessed using a hardware token, in the event an unintended user acquires the token (such as by stealing it or finding a token that was lost by its intended user) and tries to access the system with it. Exemplary apparatus and methods are illustrated in FIGs. 1, 3, 4A, and 4B, and are described especially at page 5, line 15 through page 7, line 10; page 7, line 15 through page 8, line 3; and page 9, line 21 through page 12, line 26. One or more specific host computer(s) (102) are initially set up to work in conjunction with the token (150A, 150B). That is done (for example, when the token is first coupled to the host) by generating a non-varying fingerprint F of the host (304), combining an identifier P securing access to the token (such as a PIN/password stored on the token, page 4 lines 3-4) with the host fingerprint F to calculate a value X (306), and storing X on the host (310).

The fingerprint F is computed from non-varying host information C based on one or more unique characteristics of the host, such as hardware information like a serial number of a host processor or hard drive, a host NIC MAC address, or the like (page 7, line 15 to page 8, line 2; page 9, lines 25-30). The token can thereafter be authenticated/unlocked for use with the host (for example, after the token is decoupled from the host and later coupled again) by using the value X and the fingerprint F to regenerate the identifier P, and sending P to the token. For example, when the token is again coupled to the host after they are set up to work together, the host can retrieve the value X from its storage (314), recompute the fingerprint F from its own non-varying information C (312), recover P from X using F (316), and send P to the token to unlock the token (318). A user may then, for example, use other information stored on the token,

such as login credentials, to gain access to the computer system. Thus, the fingerprint of the host is not stored in the token, and the token cannot be used to gain access to the secured computer system or data except in conjunction with the host(s) it is set up to work with.

Independent claim 34 recites a method of authenticating a hardware token for operation with a host (page 9, line 25 to page 10, line 27), comprising:

retrieving a value X from a memory separate from the token accessible to an authenticating entity ((314), page 10, lines 15-17), the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the token (page 10, lines 6-7), wherein the host fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host (page 7, line 16 to page 8, line 2; page 9, lines 26-30);

regenerating the same identifier value P at least in part from the value X and the fingerprint F ((316), page 10, lines 20-25); and

transmitting the regenerated identifier P to the token to authenticate the token for operation with the host ((318), page 10, lines 25-27).

Independent claim 49 recites an apparatus (FIG. 1; page 5, line 14 to page 7, line 10; page 9, line 25 to page 10, line 27) for authenticating a hardware token (150A, 150B) for operation with a host (102), comprising:

means (102, 134) for retrieving a value X from a memory separate from the token (106, 120, 124, 134) accessible to an authenticating entity (102, 134), the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the token,

wherein the host fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host;

means (102, 134) for regenerating the same identifier value P at least in part from the value X and the fingerprint F; and

means (102, 130, 152) for transmitting the regenerated identifier P to the token to authenticate the token for operation with the host.

Independent claim 64 recites an apparatus (FIG. 1; page 5, line 14 to page 7, line 10; page 9, line 25 to page 10, line 27) for authenticating a hardware token (150A, 150B) for operation with a host (102), the apparatus comprising a processor and a memory storing instructions for performing steps comprising the steps of:

retrieving a value X from a memory separate from the token accessible to an authenticating entity ((314), page 10, lines 15-17), the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the token (page 10, lines 6-7), wherein the host fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host (page 7, line 16 to page 8, line 2; page 9, lines 26-30);

regenerating the same identifier value P at least in part from the value X and the fingerprint F ((316), page 10, lines 20-25); and

transmitting the regenerated identifier P to the token to authenticate the token for operation with the host ((318), page 10, lines 25-27).

## **6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

The grounds of rejection to be reviewed on appeal are:

- a. the rejection of claims 49 and 51-63 under 35 USC § 101 as being allegedly directed to non-statutory subject matter and as directed to software per se;
- b. the rejection of claims 34, 38-44, 49, 53-59, 64, and 68-74 under 35 USC § 103(a) as being allegedly unpatentable over Iijima (US Patent 5,225,664) in view of Ho et al. (US PG Pubs 20030143989 A1) and Caci et al. (US Pub. 2007/0145125 A1);
- c. the rejection of claims 45-48, 60-63, and 75-78 under 35 USC § 103(a) as being allegedly unpatentable over Iijima (same as above), Ho (same as above), and Caci (same as above), in view of Miura (US Patent No. 6,952,775); and
- d. the rejection of claims 36-37, 51-52, and 66-67 under 35 USC § 103(a) as being allegedly unpatentable over Iijima (same as above), Ho (same as above), and Caci (same as above) in view of Ayyagari et al. (US 2003/0208677).

## **7. ARGUMENT**

### **a. 35 USC § 101 rejection of claims 49 and 51-63**

Claims 49 and 51-63 stand rejected under 35 USC § 101. The examiner's position is that those claims are directed to non-statutory subject matter as failing to fall within a statutory category and as being directed to software per se. The examiner contends that, although the preambles of those claims recite an apparatus, that does not inherently mean that the claims are directed to a machine. The examiner also contends that the specification on page 8, line 12 through page 9, line 20 describes the means for retrieving, generating, and transmitting as software, and that therefore the rejected claims are software per se.

The examiner initially rejected those claims under section 101 in the Office Action mailed July 24, 2008. In the applicants' reply to that Action, it was pointed out to the examiner that the rejected claims each recite an apparatus comprising means for performing certain recited functions. Such claims are in a means-plus-function form that is statutorily permitted. 35 USC 112, paragraph 6, states: "An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof." Each of the rejected claims contains elements as a means for performing specified functions, in accordance with 35 USC 112, and therefore recites a statutory apparatus.

It was also pointed out to the examiner that the cited passage, page 8, line 12 through page 9, line 20, does not disclose the means for retrieving, generating and transmitting as software alone. Instead, the cited passage is replete with references to a host computer, a hardware token, and a server, all performing certain described functions, but does not describe the means for retrieving, generating and transmitting as software. Furthermore, even if it were true that the cited passage, in addition to describing the operation and interaction of those elements, somehow suggested that the same functions could alternatively be accomplished purely in software (which it does not), it would be improper for the examiner to import such a limitation from the specification into the claims. MPEP 2111.01 (II).

The examiner's response to those arguments, as stated on page 2 of the final Office Action mailed February 6, 2009 under the heading "Response to Arguments," is that "the means plus functions are not tangible and/or the specification does not specifically describe the structures of that (*sic*) perform the means plus functions as being implemented by hardware

structure,” apparently because, the examiner maintains, the specification on page 8, line 13 through page 9, line 20 does describe means for retrieving, generating, and transmitting as software. Therefore, the examiner contends, the rejection is proper and is maintained.

The rejection is wrong in law. The examiner appears to confound an apparatus claim, which unquestionably falls within the scope of patentable subject matter (as a machine, manufacture, or composition of matter) with a process claim, which may not. Nevertheless, even a process claim is patent-eligible under section 101 if it is tied to a particular machine or apparatus. Gottschalk v. Benson, 409 U.S. 63, 70 (1972). Referring to claim 49, it can be seen that the recited means are indeed tied to tangible elements, such as a hardware token, a host, and a memory separate from the token. Therefore, even if claim 49 was a process claim, which it is not, it would not be excluded from patentability under section 101, because it is tied to a particular machine or apparatus.

Furthermore, as applicants pointed out in the reply to the previous Action, the cited portion of the specification is replete with references to a host computer, a hardware token, and a server, all performing certain described functions, but does not disclose the claimed means for retrieving, regenerating, and transmitting as software. The examiner was requested, should the examiner continue to maintain that it does, to quote the exact portion and cite the precise location where that description exists. The examiner did not do so.

Moreover, even if it were true that the specification disclosed the claimed means as being software (which it does not), it would still be understood by one of ordinary skill in the art that the means would necessarily also include hardware sufficient to run the software and to cause the associated hardware to perform the functions described, and could not possibly be simply software *per se*.



The arguments above were presented to the examiner in a reply after final rejection that contained no amendments, requesting that the rejection be reconsidered and withdrawn. In a telephone conference on April 1 initiated by the examiner, the examiner and applicants' counsel discussed certain claim amendments proposed by the examiner. The examiner on April 1 provided via email a partial copy of the amendments discussed, including only suggested amendments to the independent claims, attached hereto as Appendix A. Later on April 1, the examiner provided via email a complete copy of the proposed amendments, including highlighted newly proposed suggested amendments, attached hereto as Appendix B. On April 2 another telephone conference was held between the examiner and applicants' counsel, but no agreement was reached, and an advisory action was mailed on April 7, 2009. The advisory action cites to an interview summary "done on April 2, 2009," but mailed on April 8, 2009. The interview summary includes the text of the examiner's proposed amendments. Therefore, the examiner's proposed amendments are understood to be part of the record. However, because the interview summary does not include underline or strikethrough indicators showing the additions or deletions, respectively, proposed by the examiner, it is not an accurate reflection of the proposed amendments. Therefore, the examiner-proposed amendments mentioned above have been included in the appendices.

The examiner did not attempt to challenge the arguments against the section 101 rejection presented above, either in the telephone conference or in the Advisory Action. Instead, the Advisory Action indicates the arguments in the response after final are deemed not persuasive because "the applicant's undersigned attorney Gregory J. Lavorgna admitted that the 101 rejection is proper and he agreed with the examiner's proposed amendment or (*sic*) adding 'a memory' will solve the problem." (Advisory Action mailed April 7, 2009, page 2.) That is

incorrect. On the contrary, applicants' counsel's stated position was that the amendment suggested by the examiner to overcome the section 101 rejection should not be necessary because the rejection is without merit, but would be acceptable if deemed by the examiner to place those claims in condition for allowance because the suggested amendment had no effect on the scope of the claims. Specifically, the relevant proposed examiner's amendment consisted of the addition to claim 49, immediately after the preamble, of the element "a memory." This proposed amendment is believed to be moot, because the very next clause of claim 49 as presented already recites "means for retrieving a value X from a memory ...."

Based on the remarks presented above, it is clear that the rejection of claims 49, and 51-63 under 35 USC § 101 is without merit, and should be reversed.

**b. 35 USC § 103 rejection of claims 34, 38-44, 49, 53-59, 64, and 68-74**

Claims 34, 38-44, 49, 53-59, 64, and 68-74 were rejected under 35 USC § 103(a) as being allegedly unpatentable over Iijima (US Patent 5,225,664) in view of Ho et al. (US PG Pubs 20030143989 A1) and Caci et al. (US Pub. 2007/0145125 A1).

Regarding claims 34, 49, and 64, the examiner admits (final Office Action mailed February 6, 2009, page 5) that the combination of Iijima and Ho fails to disclose retrieving a value X from a memory separate from a token accessible to an authenticating entity, wherein the value X is generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the token, wherein the host fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host. The examiner relies on Caci for those features, citing paragraphs 51-54, claim 1, and figs. 8 and 11. However, Caci does not disclose or suggest those features, at the cited locations or elsewhere. Instead, at the cited

locations, Caci teaches misaligning a memory location address of a memory in a handheld appliance (which the claims do not recite) based on a generated random number (which the claimed method does not use), aligning the memory location address only when a smart card is inserted into the appliance (which the claims do not recite), and properly storing and retrieving private information to and from the misaligned memory location only when the card is inserted into the appliance (which the claims do not recite), thereby making the private information unavailable when the card is not inserted. That passage simply has nothing to do with the claimed features the examiner contends are found there.

Specifically, in the advisory action the examiner contends that “Caci discloses a method of unlocking access to encrypted random access memory (RAM) when a smart card is inserted into the smart card reader of a handheld device, unlocking access is granted when a secure data hash on the handheld device matches with a hash stored on the smart card, to process unlocking access personal identification number or other smart card information and unique information is received and accessed from the smart card reader of the handheld device,” again citing paragraphs 51-54, claim 1, and figs. 8 and 11. However, that is not what is recited in the claims.

Notably, however, prior to those steps, Caci teaches that a user enters a PIN when the smart card is inserted into the appliance to unlock the card. “The user is prompted to enter a personal identification number (PIN) 31. The user’s PIN number 31 is verified 32S with the PIN 30 stored in the smart card,” Caci, paragraph 48, lines 4-6. Caci does not disclose or suggest, at the cited location or elsewhere, generating a non-varying computer fingerprint based on a unique characteristic of a host as claimed, such as a unique processor serial number, NIC MAC address, BIOS code area checksum, or the like (as described at page 7, line 16 through page 8, line3), in

order to regenerate an identifier P (such as a PIN) and transmit it to the token (such as a smartcard), whereby the user does not enter a PIN.

In accordance with the claims, in a setup phase (e.g., when a hardware token is initially coupled to a host), a value X is generated from both a fingerprint F of the host and an identifier P (such as a PIN) of the hardware token. The fingerprint F is computed from non-varying host information C based on unique characteristics of the host. The value X is stored in a memory separate from the token (e.g., on the host), but is not stored on the token. Thereafter (e.g., when the token is later coupled again to the host), the value X is retrieved from the memory separate from the token, and the host fingerprint F is obtained (preferably in the same way it was originally computed). The value P is regenerated from X and F, and is transmitted to the token to authenticate the token for operation with the host, i.e., to unlock the token for use with the host. Thus, the end result of the claims is that the value P is automatically and securely regenerated and transmitted to the token, which can only be accomplished by a specific host that was previously set up to do so in conjunction with a specific token. The user does not enter P; rather, the user simply couples the token to the host, and the host regenerates P from X and F and automatically uses it to unlock the token. Thereafter, information stored on the token is accessible, such as, for example, logon credentials of the user stored on the token that can be accessed to log the user onto a secure computer system. In this way, a user need not remember, and indeed need not ever even know, the token identifier P; yet the token can be used to store information securely which can only be accessed when the token is coupled to a host it is explicitly set up to work with.

In other words, as recited in claim 34 (claims 49 and 64 are similar), the token is authenticated for operation with the host by “retrieving a value X from a memory separate from

the token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the token, wherein the host fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host; regenerating the same identifier value P at least in part from the value X and the fingerprint F; and transmitting the regenerated identifier P to the token to authenticate the token for operation with the host.”

In contrast, in the cited material in Caci, a smart card (analogous to the claimed token) is inserted into a handheld device (analogous to the claimed host), and the user enters a PIN to unlock the smart card. “... receiving a user entry including a candidate personal identification number,” Caci, claim 1, lines 15-16. In stark contrast, in the present claims the user does not enter a PIN to unlock the token. Rather, a host that has been set up to work with the token automatically recovers the PIN and automatically uses it to unlock the token.

In connection with the subject matter of the claims, there is nothing novel about inserting a smart card into a device and entering a PIN to access secured information as taught by Caci. Thereafter in Caci, after the user has entered the PIN to unlock the smartcard, a secure data hash on the handheld device is compared with a hash stored on the smart card. That might arguably be interpreted as somewhat analogous to one possible use of a token authenticated in accordance with the claims, i.e., using logon credentials stored on a token to log the user onto a secure computer system, as mentioned previously. However, those steps are not included in the recitation of the instant independent claims.

Thus, the examiner admits that Iijima combined with Ho does not disclose the features discussed above, and Caci also does not disclose or suggest these features, which are present in claims 34, 49, and 64. For at least that reason, the rejection of those claims under 35 USC §

103(a) is not supported, and should be reversed. Claims 38-44 depend from claim 34, claims 53-59 depend from claim 49, and claims 68-74 depend from claim 64, and the rejection of those claims under section 103 is not supported for at least the same reasons as their base claims, and should also be reversed.

The examiner contends in the advisory action that applicants had argued that Caci “fail[s] to teach unique characteristics of a host as claimed,” advisory action page 2, line 14. That is incorrect. Instead, applicants had argued in the response after final Action that “Caci does not disclose or suggest, at the cited location or elsewhere, generating a non-varying computer fingerprint based on a unique characteristic of a host as claimed,” (reply to final Office Action, page 4, lines 5-6). In the advisory action, the examiner contends that the “applied references” disclose “unique information of a device” as claimed. However, the examiner makes no attempt to cite where exactly in the dozens of pages of the applied references that material is found. Furthermore, the examiner does not disagree with applicants’ argument that Caci does not suggest generating a non-varying computer fingerprint based on a unique characteristic of the host as claimed.

**c. 35 USC § 103 rejection of claims 45-48, 60-63, and 75-78**

Claims 45-48, 60-63, and 75-78 were rejected under 35 USC § 103(a) as being allegedly unpatentable over Iijima (same as above) combined with Ho (same as above) and Caci (same as above), in view of Miura (US Patent No. 6,952,775).

Claims 45-48, 60-63, and 75-78 depend from claims 34, 49, and 64, respectively, and it is noted that Miura is relied on only for the additional features of claims 45-48, 60-63, and 75-78. Miura does not supplement Iijima combined with Ho and Caci to provide the features of claims

34, 49, and 64 missing therefrom, as discussed above. Therefore, the section 103 rejection of claims 45-48, 60-63, and 75-78 is not supported for at least the same reasons the rejection of their base claims is not supported, and the rejection of those claims should also be reversed.

**d. 35 USC § 103 rejection of claims 36-37, 51-52, and 66-67**

Claims 36-37, 51-52, and 66-67 were rejected under 35 USC § 103(a) as being allegedly unpatentable over Iijima (same as above) combined with Ho (same as above) and Caci (same as above) in view of Ayyagari et al. (US 2003/0208677).

Claims 36-37, 51-52, and 66-67 depend from claims 34, 49, and 64, respectively, and it is noted that Ayyagari is relied on only for the additional features of claims 36-37, 51-52, and 66-67. Ayyagari does not supplement Iijima combined with Ho and Caci to provide the features of claims 34, 49, and 64 missing therefrom. Therefore, the section 103 rejection of claims 36-37, 51-52, and 66-67 is not supported for at least the same reasons the rejection of their base claims is not supported, and the rejection of those claims should also be reversed.

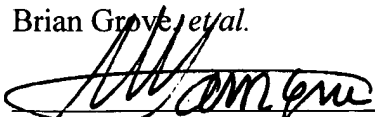
**viii. Conclusion**

Based on the arguments presented above, Appellants respectfully request that the Board reverse the examiner's rejection of claims 34, 36-49, 51-64, and 66-78.

Respectfully submitted,

Brian Grove, *et al.*

BY:

  
GREGORY J. LAVORGNA  
Registration No. 30469  
Drinker Biddle & Reath LLP  
One Logan Square  
18<sup>th</sup> and Cherry Streets  
Philadelphia, PA 19103-6996  
Tel: 215-988-3309  
Fax: 215-988-2757  
*Attorney for Applicant*



## **8. CLAIMS APPENDIX**

1. (Withdrawn) A method of authenticating a hardware token, comprising the steps of:

generating a host fingerprint F;

transmitting the fingerprint to an authorizing device;

receiving a random value R from the authorizing device;

computing a challenge R', the challenge R' derived at least in part from the fingerprint F and a random number R;

transmitting the challenge R' to the hardware token;

receiving a response X from the hardware token, the response X generated at least in part from the challenge R'; and

transmitting the response X to the authorizing device.

2. (Withdrawn) The method of claim 1, wherein the step of generating the fingerprint comprises the steps of:

collecting host information C; and

forming the fingerprint F at least in part from the host information C.

3. (Withdrawn) The method of claim 2, wherein the step of forming the fingerprint F from the host information C comprises the step of hashing the host information C.

4. (Withdrawn) The method of claim 2, wherein:

the method further comprises the step of receiving authorizing device specific value V;

and

the step of forming the fingerprint F at least in part from the host information C comprises the step of forming the fingerprint F at least in part from the host information C and the authorizing device specific value V.

5. (Withdrawn) The method of claim 4, wherein the step of forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprises the step of forming the fingerprint F at least in part from a hash of the host information C and the authorizing device specific value V.

6. (Withdrawn) The method of claim 4, wherein the step of forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprises the step of forming the fingerprint F at least in part from a concatenation of the host information C and the authorizing device specific value V.

7. (Withdrawn) The method of claim 2, wherein the host comprises a computer communicatively coupleable to the authorizing device and the hardware token, and the host information C includes information selected from the group comprising:

- processor serial number;
- hard drive serial number;
- network interface MAC address;
- BIOS code checksum;
- operating system; and
- system directory timestamp.

8. (Withdrawn) The method of claim 1, further comprising the step of:  
receiving an authentication message from the authorizing device if the transmitted response X matches an expected response X' generated by the authenticating device at least in part from the fingerprint F and the random number R.

9. (Withdrawn) The method of claim 1, wherein the response X is generated from a shared secret S between the authorizing device and the hardware token.

10. (Withdrawn) The method of claim 9, wherein the response X is the challenge R' encrypted by the shared secret S.

11. (Withdrawn) The method of claim 1, wherein the response X is generated from a private key  $K_{pr}$  of a of a key pair having the private key  $K_{pr}$  accessible to the token and a public key  $K_{pu}$  accessible to the authorizing device.

12. (Withdrawn) An apparatus for authenticating a hardware token, comprising:  
means for generating a host fingerprint F;  
means for transmitting the fingerprint to an authorizing device;  
means for receiving a random value R from the authorizing device;  
means for computing a challenge R', the challenge R' derived at least in part from the fingerprint F and a random number R;  
means for transmitting the challenge R' to the hardware token;

means for receiving a response X from the hardware token, the response X generated at least in part from the challenge R'; and

means for transmitting the response X to the authorizing device.

13. (Withdrawn) The apparatus of claim 12, wherein the means for generating the fingerprint comprises:

means for collecting host information C; and

means for forming the fingerprint F at least in part from the host information C.

14. (Withdrawn) The apparatus of claim 13, wherein the means for forming the fingerprint F from the host information C comprises means for hashing the host information C.

15. (Withdrawn) The apparatus of claim 13, wherein:

the apparatus further comprises means for receiving authorizing device specific value V;

and

the means for forming the fingerprint F at least in part from the host information C comprises means for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V.

16. (Withdrawn) The apparatus of claim 15, wherein the means for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprises means for forming the fingerprint F at least in part from a hash of the host information C and the authorizing device specific value V.

17. (Withdrawn) The apparatus of claim 15, wherein the means for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprises the means for forming the fingerprint F at least in part from a concatenation of the host information C and the authorizing device specific value V.

18. (Withdrawn) The apparatus of claim 13, wherein the host comprises a computer communicatively coupleable to the authorizing device and the hardware token, and the host information C includes information selected from the group comprising:

- processor serial number;
- hard drive serial number;
- network interface MAC address;
- BIOS code checksum;
- operating system; and
- system directory timestamp.

19. (Withdrawn) The apparatus of claim 12, further comprising:  
means for receiving an authentication message from the authorizing device if the transmitted response X matches an expected response X' generated by the authenticating device at least in part from the fingerprint F and the random number R.

20. (Withdrawn) The apparatus of claim 12, wherein the response X is generated from a shared secret S between the authorizing device and the hardware token.

21. (Withdrawn) The apparatus of claim 20, wherein the response X is the challenge R' encrypted by the shared secret S.

22. (Withdrawn) The apparatus of claim 12, wherein the response X is generated from a private key  $K_{pr}$  of a key pair having the private key  $K_{pr}$  accessible to the token and a public key  $K_{pu}$  accessible to the authorizing device.

23. (Withdrawn) A computer for authenticating a hardware token, the computer having a processor communicatively coupled to a memory storing instructions for performing steps of:

- generating a host fingerprint F;
- transmitting the fingerprint to an authorizing device;
- receiving a random value R from the authorizing device;
- computing a challenge R', the challenge R' derived at least in part from the fingerprint F and a random number R;
- transmitting the challenge R' to the hardware token;
- receiving a response X from the hardware token, the response X generated at least in part from the challenge R'; and
- transmitting the response X to the authorizing device.

24. (Withdrawn) The apparatus of claim 23, wherein the instructions for generating the fingerprint comprise instructions for performing steps of:

collecting host information C; and

forming the fingerprint F at least in part from the host information C.

25. (Withdrawn) The apparatus of claim 24, wherein the instructions for forming the fingerprint F from the host information C comprise instructions for hashing the host information C.

26. (Withdrawn) The apparatus of claim 24, wherein:  
the computer further receives an authorizing device specific value V; and  
the instructions for forming the fingerprint F at least in part from the host information C comprise instructions for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V.

27. (Withdrawn) The apparatus of claim 26, wherein the instructions for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprise instructions for forming the fingerprint F at least in part from a hash of the host information C and the authorizing device specific value V.

28. (Withdrawn) The apparatus of claim 26, wherein the instructions for forming the fingerprint F at least in part from the host information C and the authorizing device specific value V comprise instructions for forming the fingerprint F at least in part from a concatenation of the host information C and the authorizing device specific value V.

29. (Withdrawn) The apparatus of claim 24, wherein the host comprises a computer communicatively coupleable to the authorizing device and the hardware token, and the host information C includes information selected from the group comprising:

- processor serial number;
- hard drive serial number;
- network interface MAC address;
- BIOS code checksum;
- operating system; and
- system directory timestamp.

30. (Withdrawn) The apparatus of claim 23, wherein the instructions further comprise: instructions for receiving an authentication message from the authorizing device if the transmitted response X matches an expected response X' generated by the authenticating device at least in part from the fingerprint F and the random number R.

31. (Withdrawn) The apparatus of claim 23, wherein the response X is generated from a shared secret S between the authorizing device and the hardware token.

32. (Withdrawn) The apparatus of claim 31, wherein the response X is the challenge R' encrypted by the shared secret S.



33. (Withdrawn) The apparatus of claim 23, wherein the response X is generated from a private key  $K_{pr}$  of a of a key pair having the private key  $K_{pr}$  accessible to the token and a public key  $K_{pu}$  accessible to the authorizing device.

34. (Previously Presented) A method of authenticating a hardware token for operation with a host, comprising:

retrieving a value X from a memory separate from the token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the token, wherein the host fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host;

regenerating the same identifier value P at least in part from the value X and the fingerprint F; and

transmitting the regenerated identifier P to the token to authenticate the token for operation with the host.

35. Canceled

36. (Previously Presented) The method of claim 34, wherein the host fingerprint F is computed at least in part from host information C and a non-varying server specific value V.

37. (Previously Presented) The method of claim 34, wherein the host fingerprint F is computed at least in part from host information C, a non-varying server specific value V and a non-varying string Z.

38. (Original) The method of claim 34, wherein the value X is computed in the token.
39. (Original) The method of claim 34, wherein the value X is computed according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ .
40. (Original) The method of claim 39, wherein  $f(P, F)$  comprises  $P \text{ XOR } F$ .
41. (Original) The method of claim 34, wherein the value X is further computed at least in part from a user identifier U.
42. (Original) The method of claim 41, wherein the value X is computed according to  $X = f(P, U, F)$ , wherein  $f(P, U, F)$  is a reversible function such that  $f(f(P, U, F), U, F) = P$ .
43. (Original) The method of claim 42, wherein  $f(P, U, F)$  is  $P \text{ XOR } U \text{ XOR } F$ .
44. (Original) The method of claim 34, wherein:  
the authorizing entity is a host computer communicatively coupleable to the token; and  
the value X is stored in the host computer.
45. (Original) The method of claim 34, wherein the value X is stored in a memory accessible to the authentication entity by performing steps comprising the steps of:  
computing a reference value H associated with the value X; and

associably storing the value X and the reference value H in a memory of the token.

46. (Original) The method of claim 45, wherein the step of retrieving the value X comprises the steps of:

computing the reference value H at least in part from the fingerprint F; and

retrieving the value X associated with the reference value H

47. (Original) The method of claim 46, wherein the step of computing the reference value H at least in part from the fingerprint F comprises the step of computing H as a hash of the fingerprint F.

48. (Original) The method of claim 45, wherein the reference value H is computed at least in part from a hash of the fingerprint F.

49. (Previously Presented) An apparatus for authenticating a hardware token for operation with a host, comprising:

means for retrieving a value X from a memory separate from the token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the token, wherein the host fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host;

means for regenerating the same identifier value P at least in part from the value X and the fingerprint F; and

means for transmitting the regenerated identifier P to the token to authenticate the token for operation with the host.

50. Canceled

51. (Previously Presented) The apparatus of claim 49, wherein the host fingerprint F is computed at least in part from host information C and a non-varying server specific value V.

52. (Previously Presented) The apparatus of claim 49, wherein the host fingerprint F is computed at least in part from host information C, a server specific value V and a non-varying string Z.

53. (Original) The apparatus of claim 49, wherein the value X is computed in the token.

54. (Original) The apparatus of claim 49, wherein the value X is computed according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ .

55. (Original) The apparatus of claim 54, wherein  $f(P, F)$  comprises  $P \text{ XOR } F$ .

56. (Original) The apparatus of claim 49, wherein the value X is further computed at least in part from a user identifier U.

57. (Original) The apparatus of claim 56, wherein the value X is computed according to  $X = f(P, U, F)$ , wherein  $f(P, U, F)$  is a reversible function such that  $f(f(P, U, F), U, F) = P$ .

58. (Original) The apparatus of claim 57, wherein  $f(P, U, F)$  is  $P \text{ XOR } U \text{ XOR } F$ .

59. (Original) The apparatus of claim 49, wherein:

the authorizing entity is a host computer communicatively coupleable to the token; and  
the value X is stored in the host computer.

60. (Original) The apparatus of claim 49, wherein the value X is stored in a memory of the hardware token, and wherein the hardware token further comprises:

means for computing a reference value H associated with the value X; and

means for associably storing the value X and the reference value H in a memory of the token.

61. (Original) The apparatus of claim 60, wherein the means for retrieving the value X comprises:

means for computing the reference value H at least in part from the fingerprint F; and

means for retrieving the value X associated with the reference value H.

62. (Original) The apparatus of claim 61, wherein the means for computing the reference value H at least in part from the fingerprint F comprises means for computing H as a hash of the fingerprint F.

63. (Original) The apparatus of claim 60, wherein the reference value H is computed at least in part from a hash of the fingerprint F.

64. (Previously Presented) An apparatus for authenticating a hardware token for operation with a host, the apparatus comprising a processor and a memory storing instructions for performing steps comprising the steps of:

retrieving a value X from a memory separate from the token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the token, wherein the host fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host;

regenerating the same identifier value P at least in part from the value X and the fingerprint F; and

transmitting the regenerated identifier P to the token to authenticate the token for operation with the host.

65. Canceled

66. (Previously Presented) The apparatus of claim 64, wherein the host fingerprint F is computed at least in part from host information C and a non-varying server specific value V.

67. (Previously Presented) The apparatus of claim 64, wherein the host fingerprint  $F$  is computed at least in part from host information  $C$ , a server specific value  $V$  and a non-varying string  $Z$ .

68. (Original) The apparatus of claim 64, wherein the value  $X$  is computed in the token.

69. (Original) The apparatus of claim 64, wherein the value  $X$  is computed according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ .

70. (Original) The apparatus of claim 69, wherein  $f(P, F)$  comprises  $P \text{ XOR } F$ .

71. (Original) The apparatus of claim 64, wherein the value  $X$  is further computed at least in part from a user identifier  $U$ .

72. (Original) The apparatus of claim 71, wherein the value  $X$  is computed according to  $X = f(P, U, F)$ , wherein  $f(P, U, F)$  is a reversible function such that  $f(f(P, U, F), U, F) = P$ .

73. (Original) The apparatus of claim 72, wherein  $f(P, U, F)$  is  $P \text{ XOR } U \text{ XOR } F$ .

74. (Original) The apparatus of claim 64, wherein:

the authorizing entity is a host computer communicatively coupleable to the token; and

the value  $X$  is stored in the host computer.

75. (Original) The apparatus of claim 64, wherein the value X is stored in a memory of the hardware token, and the processing steps further comprise the steps of:

- computing a reference value H associated with the value X; and
- associably storing the value X and the reference value H in a memory of the token.

76. (Original) The apparatus of claim 75, wherein the instructions for retrieving the value X comprise instructions for performing steps comprising the steps of:

- computing the reference value H at least in part from the fingerprint F; and
- retrieving the value X associated with the reference value H.

77. (Original) The apparatus of claim 76, wherein the instructions for computing the reference value H at least in part from the fingerprint F comprises instructions for computing H as a hash of the fingerprint F.

78. (Original) The apparatus of claim 75, wherein the reference value H is computed at least in part from a hash of the fingerprint F.



## **9. EVIDENCE APPENDIX**

None. No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the Examiner is being submitted.

**10. RELATED PROCEEDINGS APPENDIX**

None. There are no related proceedings.

## APPENDIX A

**From:** Shiferaw, Eleni A. (AU2136) [mailto:Eleni.Shiferaw@USPTO.GOV]  
**Sent:** Wednesday, April 01, 2009 11:56 AM  
**To:** Lavorgna, Gregory J.  
**Subject:**



**Eleni A. Shiferaw**  
**United States Patent Office**  
**Office Phone: 571 272 3867**  
**Fax: 571 273 3867**  
**Location: Randolph 2D51**  
**Art Unit: 2436**



34. (Currently Amended) A method of authenticating a hardware token for operation with a host, comprising:

retrieving a value X from a memory separate from the hardware token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a hash of concatenated ~~computed at least in part from~~ non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server;

wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;

wherein the value X is computed in the hardware token, according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ , wherein  $f(P, F)$  further comprises P XOR F, and stored in the host;

re-computing the fingerprint F;

regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and

transmitting the regenerated identifier P to the hardware token to unlock ~~authenticate~~ the hardware token for operation with the host.

49. (Currently Amended) An apparatus for authenticating a hardware token for operation with a host, comprising:

a memory;

means for retrieving a value X from a memory separate from the hardware token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a hash of concatenated ~~computed at least in part from~~ non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server;

wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;

wherein the value X is computed in the hardware token, according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ , wherein  $f(P, F)$  further comprises P XOR F, and stored in the host;

re-computing the fingerprint F;

means for regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and

means for transmitting the regenerated identifier P to the hardware token to unlock ~~authenticate~~ the hardware token for operation with the host.

64. (Currently Amended) An apparatus for authenticating a hardware token for operation with a host, the apparatus comprising a processor and a memory storing instructions for performing steps comprising the steps of:

retrieving a value X from a memory separate from the hardware token accessible to an authenticating entity, the value X generated from a non-yawing computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a hash of concatenated ~~computed at least in part from~~ non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server;

wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;

wherein the value X is computed in the hardware token, according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ , wherein  $f(P, F)$  further comprises P XOR F, and stored in the host;

re-computing the fingerprint F;

regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and

transmitting the regenerated identifier P to the hardware token to unlock ~~authenticate~~ the hardware token for operation with the host.

## APPENDIX B

**From:** Shiferaw, Eleni A. (AU2136) [mailto:Eleni.Shiferaw@USPTO.GOV]  
**Sent:** Wednesday, April 01, 2009 2:27 PM  
**To:** Lavorgna, Gregory J.; Shiferaw, Eleni A. (AU2136)  
**Subject:** 10701029

Please look at the proposed dependent claims attached, as amended and the highlighted part (correcting antecedent basis and suggesting how to include the authentication part we discussed).

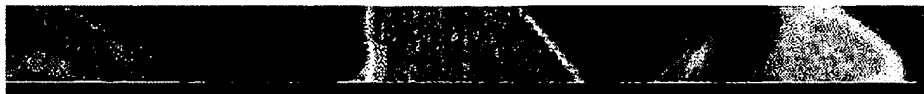
Thank you.



**Eleni A. Shiferaw**  
United States Patent Office  
Office Phone: 571 272 3867  
Fax: 571 273 3867  
Location: Randolph 2D51  
Art Unit: 2436

---

**From:** Shiferaw, Eleni A. (AU2136)  
**Sent:** Wednesday, April 01, 2009 11:56 AM  
**To:** 'gregory.lavorgna@dbr.com'  
**Subject:**





34. **(Currently Amended)** A method of authenticating a hardware token for operation with a host, comprising:

retrieving a value X from a memory separate from the hardware token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a hash of concatenated ~~computed at least in part from~~ non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server, to authenticate the hardware token;

wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;

wherein the value X is computed in the hardware token, according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ , wherein  $f(P, F)$  further comprises  $P \text{ XOR } F$ , and stored in the host;

re-computing the fingerprint F;

regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and

transmitting the regenerated identifier P to the hardware token to unlock ~~authenticate~~ the hardware token for operation with the host.

36. **(Canceled)**

38. **(Canceled)**

39. **(Canceled)**

40. **(Canceled)**

44. **(Currently amended)** The method of claim 34, wherein:

the authorizing entity is a host computer communicatively coupleable to the hardware token; and

the value X is stored in the host computer.

45. **(Currently amended)** The method of claim 34, wherein the value X is stored in a memory accessible to the authentication entity by performing steps comprising the steps of:

computing a reference value H associated with the value X; and

associably storing the value X and the reference value H in a memory of the hardware token.

48. **(Currently Amended)** The method of claim 45, wherein the reference value H is computed at least in part from ~~[[a]]~~ the hash of the fingerprint F.

49. **(Currently Amended)** An apparatus for authenticating a hardware token for operation with a host, comprising:

a memory;

means for retrieving a value X from ~~[[a]]~~ the memory separate from the hardware token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a hash of concatenated ~~computed at least in part from~~ non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server, to authenticate the hardware token;

wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;

wherein the value X is computed in the hardware token, according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ , wherein  $f(P, F)$  further comprises P XOR F, and stored in the host;

re-computing the fingerprint F;

means for regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and  
means for transmitting the regenerated identifier P to the hardware token to unlock ~~authenticate~~ the hardware token for operation with the host.

51. (Canceled)

53. (Canceled)

54. **(Canceled)**

55. **(Canceled)**

59. **(Currently amended)** The apparatus of claim 49, wherein:

the authorizing entity is a host computer communicatively coupleable to the hardware token; and

the value X is stored in the host computer.

60. **(Currently amended)** The apparatus of claim 49, wherein the value X is stored in a memory

of the hardware token, and wherein the hardware token further comprises:

means for computing a reference value H associated with the value X; and

means for associably storing the value X and the reference value H in a memory of the hardware token.

63. **(Currently Amended)** The apparatus of claim 60, wherein the reference value H is computed at least in part from [[a]] the hash of the fingerprint F.

64. **(Currently Amended)** An apparatus for authenticating a hardware token for operation with a host, the apparatus comprising a processor and a memory storing instructions for performing steps comprising the steps of:

retrieving a value X from a memory separate from the hardware token accessible to an authenticating entity, the value X generated from a non-yawing computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a

hash of concatenated ~~computed at least in part from~~ non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server, to authenticate the hardware token;

wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;

wherein the value X is computed in the hardware token, according to  $X = f(P, F)$ , wherein  $f(P, F)$  is a reversible function such that  $f(f(P, F), F) = P$ , wherein  $f(P, F)$  further comprises P XOR F, and stored in the host;

re-computing the fingerprint F;

regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and

transmitting the regenerated identifier P to the hardware token to unlock ~~authenticate~~ the hardware token for operation with the host.

66. (Canceled)

68. (Canceled)

69. (Canceled)

70. (Canceled)

74. (Currently amended) The apparatus of claim 64, wherein:

the authorizing entity is a host computer communicatively coupleable to the hardware token; and

the value X is stored in the host computer.

75. **(Currently amended)** The apparatus of claim 64, wherein the value X is stored in a memory

of the hardware token, and the processing steps further comprise the steps of:

computing a reference value H associated with the value X; and

associably storing the value X and the reference value H in a memory of the hardware token.

78. **(Currently amended)** The apparatus of claim 75, wherein the reference value H is computed at least in part from [[a]] the hash of the fingerprint F.